Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 1, January -2017

PASSMATRIX BASED SHOULDER SURFING RESISTANT GRAPHICAL AUTHENTICATION SYSTEM: Review

A. A. Ghasad [1], A. B. Deshmukh[2], A. B. Bardekar[3]

[1]*Department of Information Technology, Sipna COET, Amravati*
[2]*Assistant Professor, Department of Information Technology, Sipna COET, Amravati*
[3]*Associate Professor, Department of Information Technology, Sipna COET, Amravati*

Abstract—*Day by day with increased in PC innovation, the diverse sorts of PC wrongdoing, misrepresentation, attack additionally expanded, because of this password security and protection are assume fundamental part in PC application. So, for this we will propose a novel confirmation framework which oppose the different types of attack which happens in client account. With a one-time substantial login indicator for image, user will choose the pass-image of Passmatrix with two factor verification and login. It offers no insight for attackers to make sense of or restricted down the secret word even they direct various camera-based assaults. The proposed framework will accomplishes better imperviousness to attack while looking after ease of use.*

Keywords-*Passmatrix, Shoulder surfing and attack model, Graphical Password, Authentication.*

I. INTRODUCTION

Textual password have been the most generally utilized confirmation technique for a considerable length of time comprised of numbers and upper and lower-case letters, textual passwords are considered strong enough to resist against brute force attacks. Be that as it may, a strong textual password is difficult to retain and remember. Subsequently, users have a tendency to pick passwords that are either short or from the dictionary, as opposed to arbitrary alphanumeric strings. Surprisingly more dreadful, it is not an uncommon case that users may utilize just a single username and password for different records. As per an article in Computer world, a security group at a vast organization ran a system password cracker and shockingly split around 80% of the worker's passwords inside 30 seconds. Printed passwords are regularly unreliable because of the trouble of keeping up strong ones [1].

To keep up password we will utilize validation technique. In Two Factor Authentication used two stage confirmation and that requires a password and username as well as something that exclusive, and just, that user has on them, i.e. a bit of data just they ought to know or have quickly to hand, for example, a physical token. Utilizing a username and password together with a bit of data that exclusive the user knows makes it harder for potential intruders to gain access and steal that individual's personal information or an identity [2].

Utilizing a Two Factor Authentication process can bring down the quantity of instances of wholesale fraud on the Internet, and also phishing by means of email, on the grounds that the criminal would require more than simply the username and password subtle elements. The drawback to this security procedure is that new hardware tokens (as key dandies or card per users) should be requested, then issued and this can bring about log jams and issues for an organization's clients needing and holding up to access their own particular private information by means of this validation strategy. The tokens are likewise generally little and effectively lost so bringing about more issues for everybody when clients bring in asking for new ones. Secure Envoy hope to determine this issue with Two Factor Authentication by used cell phone SMS innovation. With more than 5 billion cell phones being used, transforming a telephone into an authentication gadget rapidly explains the need and extra cost and postponements of conveying hardware tokens. This sort of authentication can be viewed as speedier, faster and less expensive to set up and keep up crosswise over numerous network [6].

In this framework, we will utilized a safe graphical verification system named as Passmatrix based Shoulder surfing resistant graphical authentication system that will protects users from getting to be casualties of shoulder surfing attacks while contributing passwords in public through the use of one-time login pointers. A login marker will randomly create for every pass-image and will be pointless after the session ends. The login marker will gives better security against shoulder surfing attacks, since users utilize a dynamic pointer to call attention to the position of their passwords instead of tapping on the password object directly.

II. LITERATURE SURVEY

In the previous a very long while, bunches of research on password authentication has been done in the literature. They utilized "ADVANCED LOGIN SCHEME" in which they utilized a "MATRIX". The components of the

matrix will be a RANDOMLY produced set of letters in order, numerals and images "without" REPITITION and in a graphical authentication plot in which the users recognizes the pre-characterized image to demonstrate the authentication of the user. Among these propose plot, during registration the user chooses a set of image from a predefined set of images. Later on at the login time the user needs to choose the image that he had chosen during registration time to demonstrate his authentication. But this system is vulnerable to shoulder surfing [1].

Different graphical password authentication plan, were produced to address the issues and shortcomings connected with textual passwords. In light of a few reviews, for example, those in, people have a superior capacity to remember image with long term memory (LTM) than verbal representations. Image based passwords were turned out to be less demanding to recall in a few user considers. Subsequently, users can set up a complex authentication password and are capable for recalling it after quite a while regardless of the possibility that the memory is not actuated occasionally. In any case, the greater part of these image based passwords are powerless against shoulder surfing attacks (SSAs). This kind of attack either utilizes coordinate perception, for example, viewing behind someone or applies video catching procedures to get passwords, PINs, or other delicate individual information [4].

In the early days, Pass-face plan is a grid of nine faces and the user to choose image from the grid. The user picks four images of human as their password and needs to choose their pass-image from the other eight images. Since there are four users who select image as it is done four circumstances. In any case, this plan was anything but difficult to attacks by guessing or trying for number of time. Additionally studies were made on validation plans and another plan was proposed known as "Draw-a-Secret"(DAS) by Jermyn, et al. The user needs to draw a picture on the grid at the time of registration. The user needs to draw a similar picture on a 2D grid at the season of login. On the off chance that the drawing of picture touches a similar grid in a similar the same sequence the users gets authenticated. Be that as it may, this plan was inclined to shoulder surfing attack [5].

In reference Draw-a-Secret Similar to this a same plan was presented by Syukri. This authentication plan depended on the rule that the user needs to draw his signature by utilizing mouse. This plan had two phases of usage viz. the registration stage and the verification stage. At the season of enlistment the user draws a signature that is extracted by the system. At the season of enlistment the signature is taken as information and standardization is done and afterward the parameters are extricated and checking is done and the user is confirmed if the parameters get coordinated. In any case, drawing with mouse is not all that simple and genuine parameters can't be coordinated with the signature that was drawn at the registration time. This plan is inclined to falsification of signature [1].

Verifiably, two-factor authentication is not another idea but rather its utilization has turned out to be much more predominant with the computerized age we now live in. As of late as February 2011 Google declared two factor verifications online for their users, trailed by MSN and Yahoo. Many individuals most likely don't have the foggiest idea about this sort of security process is called Two-Factor Authentication and likely don't consider it when utilizing hardware tokens, issued by their bank to use with their card and a Personal Identification Number when hoping to finish Internet Banking exchanges. Just they are using the advantages of this kind of multifactor Authentication - i.e. "what they have" AND "what they know". Utilizing a Two Factor Authentication process can bring down the quantity of instances of wholesale fraud on the Internet, and additionally phishing by means of email, in light of the fact that the criminal would require more than simply the users name and password details [6].

III. ISSUE STATEMENT AND ATTACK MODEL

With the expanding measure of cell phones and web administrations, users can get to their own records to send private business messages, transfer photographs to collections in the cloud or dispatch cash from their e-financial balance at whatever time and anyplace. While signing into these administrations in public, they may open their passwords to obscure gatherings unknowingly. People with malevolent expectation could watch the entire authentication technique through ubiquitous camcorders and observation hardware, or even a rejected image on a window. Once the attacker acquires the password, they could get to individual records and that would definite represent an incredible risk to one's advantages. Shoulder surfing attacks have gained more and more attention in the past decade [3].

The accompanying records the exploration issues we might want to address in this review:

1) Time devouring.
2) The issue of how to perform verification out in the open so shoulder surfing attacks can be mitigated.
3) The issue of restricted ease of use of verification plans that can be connected to a few gadgets as it were.
4) The issue of obliging users to remember additional data or to perform additional calculation during authentication.
5) The issue of how to effectively seek correct password objects during the verification stage.
6) The security shortcoming the traditional PIN strategy.
7) The ease of getting passwords by spectators in public.

The diverse sorts of conceivable attacks are happen, for example, Word reference attack, Shoulder surfing Attacks, Key Logger Attacks which is as per the following-

1) WORD REFERENCE ATTACK**:-**

In cryptanalysis and PC security, a word reference attack such as dictionary attack is a procedure for defeating a cipher or an authentication mechanism by attempting to decide its decoding key or passphrase by attempting hundreds or in some cases a large number of likely conceivable outcomes, for example, words in a word reference.

2) SHOULDER SURFING ATTACK **:-**

In PC security, shoulder surfing attacks to utilizing direct perception procedures, for example, investigating somebody's shoulder, to get data, for example, somebody entering PIN while other watch. It is regularly used to acquire passwords, PINs, security codes, and comparative information.

3) KEY LOGGER ATTACK **:-**

Keystroke logging, often referred to as key logging or keyboard catching, is the activity of recording (or logging) the keys struck on a keyboard, commonly in covert manner so that the individual utilizing the keyboard is unaware that their activities are being observed.

IV. PASSMATRIX

To maintain a strategic distance from the distinctive sorts of attacks which is happens in user account. We will utilize graphical validation system called Passmatrix. In Passmatrix, a password comprises of just selecting pass-square per pass-image send for authentication form a sequence of n images. The image will be send by server. In the event that the If the user select incorrect region within the image then user lock. Be that as it may, primary motivation to oppose shoulder surfing attacks. Thus, the user can get pass-squares of image as send by server by basically touching at or tapping on them and same pass-square select in their gadget.

Passmatrix is made out of the accompanying parts

A) Image Separation Module
B) Horizontal and Vertical Bar Control Module
C) Login Indicator generator Module
D) Communication Module
E) Password Verification Module
F) Database

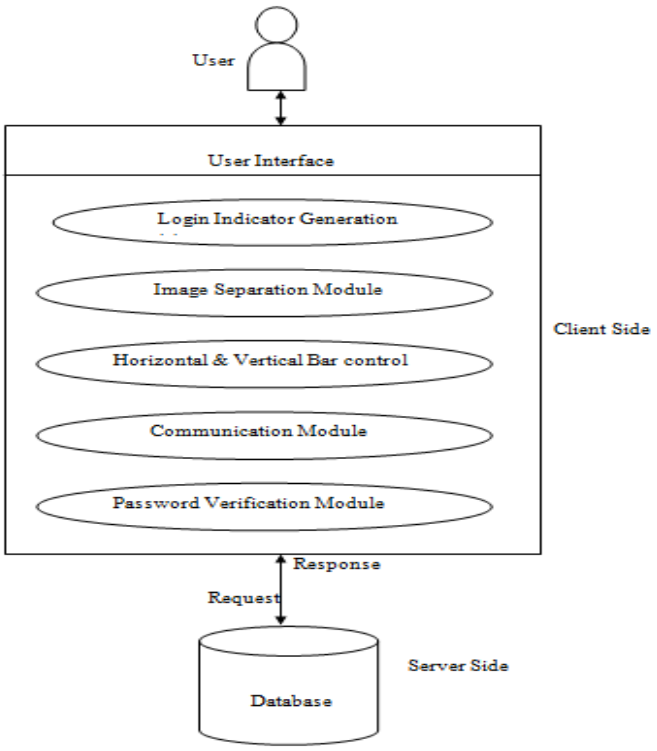

Fig. 1 Outline of the Passmatrix framework.

A) IMAGE SEPARATION MODULE**:-**

This module separates every image into squares, from which user would pick one as the pass-square, an image is partition into lattice design and randomly scattered image send by the server to users in both side web-site and cell phone.

B) LOGIN INDICATOR GENERATOR MODULE**:-**

This module creates a login pointer comprising of a few recognizable characters, (for example, letters in order and numbers) or visual materials, (for example, hues and symbols) for users during the confirmation stage. Numbers or letters are created randomly and along these lines an alternate login marker will be given every time the module is called. The produced login pointer can be given to user outwardly or acoustically. For the previous case, the indicator could be appeared on the show specifically or through another image.

C) HORIZONTAL & VERTICAL BAR CONTROL MODULE:-

There are two parchment bars: a level bar with a grouping of letters and a vertical bar with an arrangement of numbers. This control module gives drag and excursion capacities to users to control both bars. User can throw either bar utilizing their finger to move one alphanumeric at once. They can likewise move a few checks at once by dragging the bar for a separation. Both bars are circulative, i.e., if the user moves the horizontal bar in Figure 2(c) to left by three checks, it will end up being the bar appeared in Figure 2(d). The bars are utilized to verifiably bring up (or at the end of the day, adjust the login indicator to) the area of the user's pass-square.

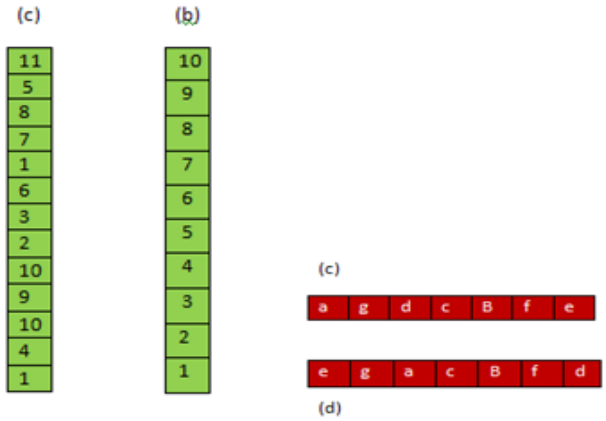

Fig.2 Horizontal bar (on right/green) and Vertical bar (on the left/red)

D) COMMUNICATION MODULE**:-**

This module is accountable for all the data transmitted between the customer gadgets and the authentication server. Any communication is protected by SSL (Secure Socket Layer) protocol and thus, is safe from being eavesdropped and intercepted.

E) PASSWORD VERIFICATION MODULE**:-**

This module checks the user password during the validation stage. Pass-square acts like a password which is send by serve. The user is validated just if every pass-square in every pass-image is effectively adjusted to the login pointer.

F) DATABASE**:-**

The database server contains a few tables cap store user accounts, passwords (ID number of pass-images and the places of pass-squares), and the time duration each user spent on both registration phase and login phase Passmatrix has all the required benefits toper form operations like insert, modify, delete and search.

V. AUTHENTICATION

Graphical password validation consists of a registration stage and an authentication stage which is as per the following.

A) REGISTRATION STAGE:-

The Figure demonstrate flow-chart of the registration stage. At this stage, the user will create an account which contains a username and a password. The main motivation behind the username will to give the user an imagination of having a personal account. The username can be overlooked if Passmatrix will connected to authentication system like screen lock. The user will give automatically image from server or uploaded image and user

will choose Passmatrix for image. Image will partition into grid and randomly scattered image will send to web-site and same image send to user cell phone. In QR code image URL will automatically created and image will send to user web application. At that point the randomly scattered image will show on web-site. In two factor verifications cell phone will scan QR code and image will download. After that server will offer direction to choose pass-square of image, for example, select 2nd row, 3rd column then user will choose pass-square and send to server. In web-site user will likewise choose a pass-square of pass-image from scattered image. In the event that chose pass-image of both sides are right then user consequently login on Home page and input send to server.

B) AUTHENTICATION STAGE **:-**

The Figure indicates flow-graph of the validation stage. At this stage, the user will utilize username, password and login indicators to sign into Passmatrix. To begin with the user will include username which will make in the registration stage and select matrix format then the server check username and grid format which utilized as a part of registration stage. Next, the server randomly scattered image and direction will be send with the assistance of a horizontal bar and a vertical bar on its top and left individually, then user will choose the pass-square of image strike direction of server. For instance, if the pointer is (E, 11) and the pass-square is at (5, 7) in the grid of the image, the user moves the character "E" to the 5th column on the horizontal bar and "11" to the 7th row on the vertical bar. The correspondence module gets user account data from the server through HttpRequest POST strategy. At last, for every image, the password verification modules will confirms the chose pass-square of both side, for example, web-site and cell phone if the pass-square will correct then login. Just if all the validation will amend in image, the client will permitted to sign into Home page [2].

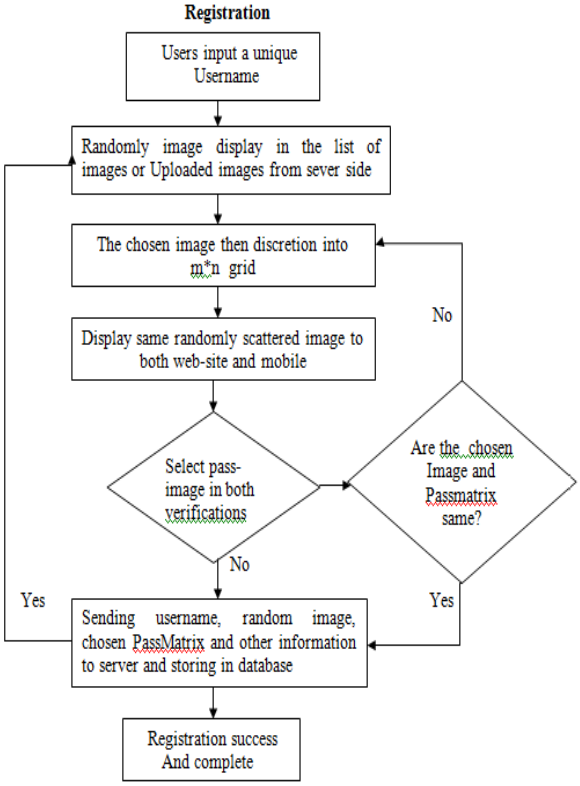

Fig.3 The flowchart of Registration Stage in Passmatrix

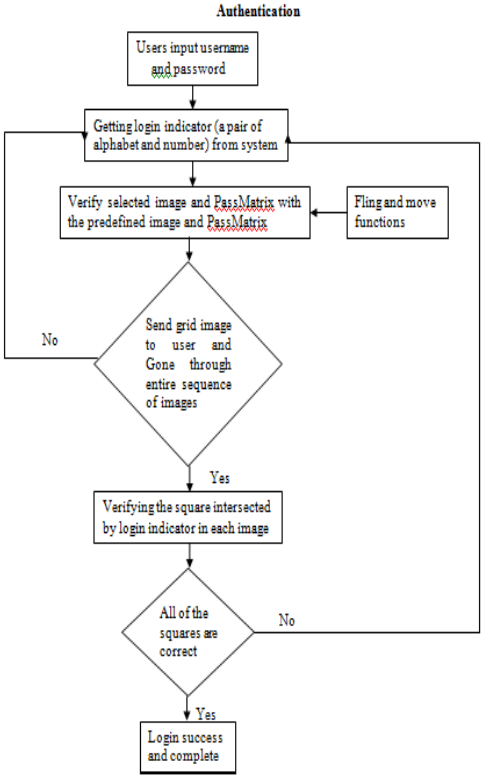

Fig. 4 The flowchart of Authentication Stage in Passmatrix

VI. GRAPHICAL PASSWORD

To overcome the security weakness of the traditional PIN technique, the effortlessness of getting passwords by observers in public, and the similarity issues to gadgets, we presented a graphical authentication system. In which, a password will consists of just by selecting pass-square of scattered image as indicated by server direction if both the side, for example, site and cell phone correct then client login. Clock begin when user login if time out client consequently logout.

CONCLUSION

In this review paper to think about Passmatrix based shoulder surfing resistant graphical authentication system. By using this application user will able to access their personal data anytime and anywhere with various device.

ACKNOWLEDGMENT

This review paper work is finished effectively simply because support from every single one including educators, companions. Extraordinarily, I am extremely appreciative to the individuals who give me direction and make this work done.

REFERENCES

[1] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh and Chia-Yun Chen, "A Shoulder Surfing Resistant Graphical Authentication System", IEEE Transaction on Dependable and secure computing,2016.

[2] S. Vaithyasubramanian, A. Christy and D. Saravanan, "Two Factor Authentications for Secured Login In Support Of Effective Information Preservation And Network Security", ARPN Journal of Engineering and Applied Sciences, VOL. 10, NO. 5, March 2015

[3] Arash Habibi Lashkari, Dr. Omar Bin Zakaria, Samaneh Farmand, Dr. Rosli Saleh, "Shoulder Surfing Attack in Graphical Password Authentication" , Int. Journal of Computer Science and Information Security,Vol. 6, No.2, 2009.

[4] Peng Foong Ho, Yvonne Hwei-Syn Kam, Mee Chin Wee, Yu Nam Chong, and Lip Yee Por, "Preventing Shoulder-Surfing Attack with the Concept of Concealing the Password Objects Information", Hindawi Publishing Corporation,The Scientific World Journal, 27 May 2014.

[5] Amish Shah, Parth Ved, Avani Deora, Arjun Jaiswal, Mitchell D'silva, "Shoulder-Surfing Resistant Graphical Password System", Int. Conf. On Advanced Computing Technologies and Applications, 2015.

[6] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones".

